

DISTRIBUTION OF THE TRACE OF FROBENIUS ON AVERAGE FOR RANK 2 DRINFELD MODULES

ABEL CASTILLO

ABSTRACT. Let q be an odd prime power, $a \in \mathbb{F}_q[T]$ and $u \in \mathbb{F}_q^*$. Provided $q \geq 17$, we compute the average number of primes p for which the characteristic polynomial of the Frobenius at p is $X^2 - aX + up$ over a family of rank 2 Drinfeld $\mathbb{F}_q[T]$ -modules. Our results give asymptotic formulas in the x -limit.

1. INTRODUCTION

Let q be a power of an odd rational prime. Let \mathbb{F} be the field with q elements. Let $A := \mathbb{F}[T]$ and $F := \mathbb{F}(T)$. Since A is a unique factorization domain, non-zero prime ideals correspond to monic irreducible polynomials in T . We always use the letter p to denote monic irreducibles in A . For $a \in A$, define $|a| := q^{\deg a}$ and $\text{sgn } a$ to be the leading coefficient of a as a polynomial in T .

Let $F\{\tau\}$ be the non-commutative polynomial ring with the commutation rule $\tau a = a^q \tau$ for all $a \in F$. A Drinfeld module (more precisely, a Drinfeld A -module) over F of rank r is given by an \mathbb{F} -algebra homomorphism $\Phi : A \rightarrow F\{\tau\}$, $n \mapsto \Phi_n$, where the image of T is

$$\Phi_T = T + c_1 \tau + \cdots + c_r \tau^r,$$

with $c_i \in F$, $c_r \neq 0$, and $r \geq 1$.

For all but finitely many monic irreducibles p in A , the reduction of Φ modulo p is a Drinfeld module over the residue field of p of rank r , and the Frobenius endomorphism at p satisfies a polynomial of degree r , which we refer to as the characteristic polynomial of Frobenius at p for Φ . This polynomial has coefficients in A , and (additive inverse of) the next-to-leading coefficient of this polynomial $a_p(\Phi)$ gives rise to interesting arithmetic questions. For instance, one can fix an element $a \in A$ and ask for the distribution of primes p for which $a_p(\Phi) = a$.

Interest in this question can be traced back to the analogous question for elliptic curves over \mathbb{Q} . In [LT76], Lang and Trotter give the following conjecture.

Conjecture 1.1. *Let E be an elliptic curve over \mathbb{Q} without complex multiplication, and fix an integer a . For $\ell \in \mathbb{N}$ a prime of good reduction, let a_ℓ be the trace of Frobenius at ℓ of E . Then,*

$$\#\{\ell \text{ prime in } \mathbb{Z}: 1 \leq \ell \leq x, a_\ell(E) = a\} \sim C_{E,a} \frac{\sqrt{x}}{\log x},$$

where $C_{E,a}$ is a constant depending only on E and a .

The conjecture remains unproven, but progress has been made in the form of upper bounds (see for instance [Ser81], [CFM05], and [MMS88]).

An approximation to this problem is to consider an average over a “box” of elliptic curves. Probably the first such computation can be found in the work of Fouvry and Murty [FM96], where they compute the average number of primes for which $a_\ell = 0$ for the two-parameter family of elliptic curves $\{E_{(a,b)} :$

$y^2 = x^2 + ax + b$. They obtain the following asymptotic formula (the dash indicates a sum over models of non-singular curves):

$$\frac{1}{4AB} \sum_{\substack{|a| \leq A \\ |b| \leq B}}' \#\{\ell \text{ prime in } \mathbb{Z}: 1 \leq \ell \leq x, a_\ell(E_{(a,b)}) = 0\} \sim \frac{\pi \sqrt{x}}{3 \log x},$$

provided $A, B > x^{\frac{1}{2}+\varepsilon}$ and $AB > x^{\frac{3}{2}+\varepsilon}$ for some $\varepsilon > 0$. More generally, one has [DP99], where David and Pappalardi fix an integer a and compute the average number of primes for which $a_\ell = a$, obtaining

$$\frac{1}{4AB} \sum_{\substack{|a| \leq A \\ |b| \leq B}}' \#\{\ell \text{ prime in } \mathbb{Z}: 1 \leq \ell \leq x, a_\ell(E_{(a,b)}) = a\} \sim C_a \frac{\sqrt{x}}{\log x},$$

with the constant C_a given explicitly, provided $A, B > x^{1+\varepsilon}$ for some $\varepsilon > 0$. Improvements to the result in [DP99] come in the form of smaller box sizes obtained through the use of character sum estimates (see for instance [Bai07] and [BS09]). For instance, Baier [Bai07] reduces the conditions on A and B to $A, B > x^{\frac{1}{2}+\varepsilon}$ and $AB > x^{\frac{3}{2}+\varepsilon}$ for some $\varepsilon > 0$.

It is natural to ask for average results such as these for rank 2 Drinfeld modules. To this effect, David [Dav96] obtains an analogue of the result of Fouvry and Murty, counting supersingular reductions for rank 2 Drinfeld modules on average. More precisely, as x runs through positive integers and $x \rightarrow \infty$,

$$\frac{1}{q^{\mathcal{A}+1}q^{\mathcal{B}+1}} \sum_{\substack{\deg g \leq \mathcal{A} \\ \deg \Delta \leq \mathcal{B}}} \#\{\ell \in A \text{ monic irreducible, } \deg \ell = x : a_\ell(E_{(a,b)}) = 0\} \sim C(x, q) \frac{q^{x/2}}{x},$$

with the constant $C(x, q)$ given explicitly in terms of q and the parity of x , and provided $\mathcal{A}, \mathcal{B} \geq x$.

In this paper we prove a generalization of this last statement for more general $a \in A$. Our character sum estimates require us to avoid very small values of q , say $q \geq 17$. Our techniques follow those of [DP99] and [Bai07], giving us lower bounds on \mathcal{A} and \mathcal{B} that improve as $q \rightarrow \infty$.

1.1. Statement of Results. For $g, \Delta \in A$, let $\Phi(g, \Delta)$ be the Drinfeld module over F determined by the homomorphism

$$\Phi(g, \Delta) : A \rightarrow F\{\tau\}, \quad T \mapsto T + g\tau + \Delta\tau^2,$$

and for a prime p of good reduction, let $a_p(g, \Delta)$ and $P_p(X, g, \Delta)$ be (respectively) the trace and the characteristic polynomial of the Frobenius at p for $\Phi(g, \Delta)$.

Fix a positive integer x , and let \mathcal{P} be the set of monic irreducible polynomials in A of degree x . Let \mathcal{A}, \mathcal{B} be positive integers; these will be constrained in terms of x . We will take an average over Drinfeld modules in a two-parameter family by taking

$$\text{Box}(\mathcal{A}, \mathcal{B}) := \{(g, \Delta) \in A \times A : \deg g < \mathcal{A}, \deg \Delta < \mathcal{B}, \Phi(g, \Delta) \text{ is a rank 2 Drinfeld module}\}.$$

We are interested in the quantity

$$S(x, \mathcal{A}, \mathcal{B}, a, u) := \frac{1}{\#\text{Box}(\mathcal{A}, \mathcal{B})} \sum_{(g, \Delta) \in \text{Box}(\mathcal{A}, \mathcal{B})} \#\{p \in \mathcal{P} : P_p(X, g, \Delta) = X^2 - aX + up\}.$$

Define C_∞ , which we view as the local factor at the prime at infinity, as

$$(1.1) \quad C_\infty := \begin{cases} \frac{1}{q^{1/2}(q-1)} & \text{if } x \text{ odd,} \\ \frac{1}{(q+1)(q-1)} & \text{if } x \text{ even.} \end{cases}$$

Our main theorem makes use of character sum estimates to allow for smaller values of \mathcal{A} and \mathcal{B} for large q .

Theorem 1.2. *Take the notation above, and assume $q \geq 17$ is fixed. Suppose that $\deg a < \frac{1}{2}x$ and that,*

$$(1.2) \quad \mathcal{A}, \mathcal{B} > \frac{\log 4}{\log q} x + \log x \quad \text{and} \quad \mathcal{A} + \mathcal{B} > \left(\frac{1}{2} + \frac{\log 16}{\log q} \right) x + \log x.$$

Then, we have

$$S(x, \mathcal{A}, \mathcal{B}, a, u) = C_\infty C(a) \frac{q^{x/2}}{x} + E(x, q);$$

where C_∞ is defined in (1.1), $C(a)$ is given by

$$\prod_{\ell|a} \left(1 - \frac{1}{|\ell|^2} \right)^{-1} \prod_{\ell \nmid a} \left(\frac{|\ell|(|\ell|^2 - |\ell| - 1)}{(|\ell|^2 - 1)(|\ell| - 1)} \right),$$

and $E(q, x)$ is $\underline{O}\left(\frac{q^{x/2}}{x}\right)$ as $x \rightarrow \infty$.

In the setting studied by [DP99], there is no analogue of the unit appearing in the definition of $S(x, \mathcal{A}, \mathcal{B}, a, u)$; our result shows that, on average, there is uniform distribution over admissible $u \in \mathbb{F}^*$. The box size we obtain is comparable to [Bai07], with the difference that, for q large enough, the factors of x appearing in the expressions in (1.2) can be made arbitrarily close to 0 and $\frac{1}{2}$ respectively.

1.2. Notation. Let q be an odd prime power, and let \mathbb{F} be the finite field with q elements. Let $A := \mathbb{F}[T]$, $A^{(1)}$ the set of monic polynomials in A , and $F := \mathbb{F}(T)$. For an element $a \in A$, let $\text{sgn } a$ denote the leading coefficient of a and $\deg a$ denote the degree of a as a polynomial in T . Write $|a| = q^{\deg a}$.

The letters p and ℓ hereafter denote monic irreducible elements of A , which we refer to as primes. If p is a prime in A , let \mathbb{F}_p be the A -field A/pA . If $a \in A$, then we write \hat{a} for the element $a \bmod p$ in \mathbb{F}_p .

Define $\varphi(\cdot)$ to be the Euler-phi function on A , i.e. $\varphi(a) := \#(A/aA)^*$. As in the classical case, φ is multiplicative and has the product expansion

$$\varphi(a) = |a| \prod_{p|a} \left(1 - \frac{1}{|p|} \right).$$

From this expansion it is straightforward to deduce the identity

$$(1.3) \quad \varphi(vw) = \varphi(v)\varphi(w) \cdot \frac{\gcd(v, w)}{\varphi(\gcd(v, w))}.$$

Fix a positive integer x , and write $\mathcal{P} := \{p \in A^{(1)} : \deg p = x\}$.

2. BACKGROUND AND PRELIMINARY LEMMAS

2.1. Drinfeld modules. We refer the reader to [Dri74], [Dri77], [Gek91], and [Ros02] for more rigorous treatments of the theory of Drinfeld modules, including proofs.

For any A -field K , let $K\{\tau\}$ be the non-commutative polynomial ring with the commutation rule $\tau\alpha = \alpha^q\tau$ for all $\alpha \in K$.

For $(g, \Delta) \in A \times A$ let $\Phi(g, \Delta)$ be the Drinfeld module over F determined by the homomorphism

$$\Phi(g, \Delta) : A \rightarrow F\{\tau\}, \quad T \mapsto T + g\tau + \Delta\tau^2.$$

If $\Delta \neq 0$, this is a rank 2 Drinfeld module. For any prime $p \nmid \Delta$, let

$$P_p(X, g, \Delta) = X^2 - a_p(g, \Delta)X + u_p(g, \Delta)p \in A[X]$$

be the characteristic polynomial of the Frobenius endomorphism at p ; recall from [Gek91] that this polynomial satisfies $\deg a_p(g, \Delta) \leq \frac{1}{2} \deg p$ and $u_p(g, \Delta)$ is a unit in A .

For $(\gamma, \delta) \in \mathbb{F}_p \times \mathbb{F}_p$ with $\delta \neq 0$, let $\phi(\gamma, \delta)$ be the Drinfeld module over \mathbb{F}_p determined by

$$\phi(\gamma, \delta) : A \rightarrow \mathbb{F}_p\{\tau\}, \quad T \mapsto \hat{T} + \gamma\tau + \delta\tau^2.$$

If $\delta \neq 0$, this is a rank two finite Drinfeld module over \mathbb{F}_p , and we write

$$P(X, \gamma, \delta) = X^2 - a(\gamma, \delta)X + u(\gamma, \delta)p$$

for the characteristic polynomial of the Frobenius endomorphism.

2.2. Orders in imaginary quadratic fields. We refer the reader to [Yu95], [Gek08] for more details and proofs.

Let E be a degree 2 extension of F ; since we assume q is odd, E must be separable. We say E is an imaginary quadratic extension of F if the prime at infinity of F does not split in E . An equivalent, more concrete characterization (see for instance [Ros02, Prop. 14.6, p. 248]) is given by writing $E = F(\sqrt{D})$ with D squarefree. Then, E is an imaginary quadratic extension if and only if $\deg D$ is odd, or $\deg D$ is even and $\text{sgn } D$ is a nonsquare in \mathbb{F}^* . Whenever $D \in A$ satisfies the above, we say D is a fundamental discriminant. If d satisfies the above except possibly the squarefree condition, we simply say that d is a discriminant.

Fix a fundamental discriminant D and let $E = F(\sqrt{D})$. Then $\mathcal{O}_E := A[\sqrt{D}]$ is the ring of integers of E . Moreover, any A -subalgebra of E with A -rank 2 is contained in \mathcal{O}_E ; we call these orders in E , with \mathcal{O}_E being the maximal order in E . As in the classical setting, there is a one-to-one correspondence between discriminants (up to multiplication by a square in \mathbb{F}^*) and orders in imaginary quadratic extensions of F , given by $d \leftrightarrow A[\sqrt{d}]$. This correspondence sends fundamental discriminants to maximal orders.

For each fundamental discriminant D , we define the Dirichlet character χ_D on A associated to $A[\sqrt{D}]$ by assigning values at primes via

$$\chi_D(\ell) := \begin{cases} 0 & \text{if } \ell \text{ is ramified in } F(\sqrt{D}), \\ 1 & \text{if } \ell \text{ splits in } F(\sqrt{D}), \\ -1 & \text{if } \ell \text{ is inert in } F(\sqrt{D}), \end{cases}$$

and extending completely multiplicatively to all of A . For each discriminant d , write $d = f^2 D$ where D is a fundamental discriminant and $f \in A^{(1)}$. Then, we define the Dirichlet character χ_d on A associated to $A[\sqrt{d}]$ by assigning values at primes via

$$\chi_d(\ell) := \begin{cases} 0 & \text{if } \ell \mid f, \\ \chi_D(\ell) & \text{otherwise} \end{cases}$$

and extending completely multiplicatively to all of A . For the Dirichlet character described above, define the L -function associated to χ_d via

$$L(s, \chi_d) := \sum_{n \in A^{(1)}} \frac{\chi_d(n)}{|n|^s} \text{ for } \operatorname{Re}(s) > 1.$$

One has (see for instance [Ros02, Ch. 2]) that this function can be expressed as a polynomial in q^{-s} of degree $\deg d$. Moreover, the Riemann Hypothesis for function fields implies that, replacing q^{-s} with X , we can write the L -function of a Dirichlet character χ on A whose conductor has degree x as

$$(2.1) \quad L(s, \chi) = \prod_{i=1}^x (1 - \alpha_i X) \text{ with } \alpha_i \in \mathbb{C}, |\alpha_i| \leq q^{1/2}.$$

We also define the class number of the order $A[\sqrt{d}]$. First we define a proper ideal $I \subset A[\sqrt{d}]$ as one that satisfies

$$\{\alpha \in E : \alpha I \subseteq I\} = A[\sqrt{d}].$$

The proper ideals of $A[\sqrt{d}]$ have unique factorization into products of proper prime ideals, and we define $h(d)$, the ideal class number of $A[\sqrt{d}]$, as the number of proper $A[\sqrt{d}]$ -ideals modulo principal ideals. From the theory of quadratic spaces (see [Yu95]), we get that, if D is a fundamental discriminant and $f \in A$ the ratio of the class numbers $h(f^2 D)$ and $h(D)$ is

$$(2.2) \quad \frac{h(f^2 D)}{h(D)} = \frac{|f|}{[A[\sqrt{D}]^* : A[\sqrt{f^2 D}]^*]} \prod_{\ell \mid f} \left(1 - \frac{\chi_D(\ell)}{|\ell|}\right).$$

For maximal orders, we have the analytic class formula from Artin's thesis ([Art24], see also [Ros02, Theorem 17.8A, p. 317]):

$$(2.3) \quad h(D) = \begin{cases} \frac{|D|^{1/2}}{q^{1/2}} L(1, \chi_D) & \text{if } \deg D \text{ odd,} \\ \frac{2|D|^{1/2}}{q+1} L(1, \chi_D) & \text{if } \deg D \text{ even and } \operatorname{sgn} D \text{ is a nonsquare in } \mathbb{F}^*. \end{cases}$$

We combine (2.2) and (2.3) in the following lemma for later reference.

Lemma 2.1. *Take the notation above and suppose that $d = f^2 D$, where D is a fundamental discriminant and f is monic. Then,*

$$h(d) = \begin{cases} \frac{|d|^{1/2}}{q^{1/2}} L(1, \chi_d) & \text{if } \deg d \text{ odd,} \\ \frac{2|d|^{1/2}}{q+1} L(1, \chi_d) & \text{if } \deg d \text{ even and } \operatorname{sgn} d \text{ is a nonsquare in } \mathbb{F}^*. \end{cases}$$

2.3. Finite Drinfeld modules of rank 2. In this section we record some lemmas regarding isomorphism classes of finite Drinfeld modules. Let p be a prime in A with $\deg p = x$.

Theorem 2.2 ([Gek08, Prop. 6.8]). *Fix $a \in A$ with $\deg a < x/2$. Let $u \in \mathbb{F}^*$, and if x is even then further assume that $-4u$ is a nonsquare in \mathbb{F}^* . The number of \mathbb{F}_p -isomorphism classes of rank 2 Drinfeld modules with characteristic polynomial of Frobenius equal to $X^2 - aX + up$ is the total number of ideal classes of the ring $A \left[\sqrt{a^2 - 4up} \right]$.*

We denote this quantity as H_p , and observe that

$$(2.4) \quad H_p = \sum_{\substack{f \in A^{(1)} \\ f^2 | a^2 - 4up}} h \left(\frac{a^2 - 4up}{f^2} \right).$$

Lemma 2.3 ([Gek08, Section 1]). *Let $\phi(\alpha, \beta)$ and $\phi(\gamma, \delta)$ be rank 2 Drinfeld modules over \mathbb{F}_p (i.e. $\beta\delta \neq 0$). Then, $\phi(\alpha, \beta)$ and $\phi(\gamma, \delta)$ are \mathbb{F}_p -isomorphic if and only if there exists $\mu \in \mathbb{F}_p^*$ such that*

$$(\alpha, \beta) = (\mu^{q-1}\gamma, \mu^{q^2-1}\delta).$$

Moreover,

$$\#\{(\alpha, \beta) : \phi(\alpha, \beta) \equiv_{\mathbb{F}_p} \phi(\gamma, \delta)\} = \begin{cases} \frac{|p|-1}{q^2-1} & \text{if } \gamma = 0 \text{ and } \deg p \text{ even,} \\ \frac{|p|-1}{q-1} & \text{otherwise.} \end{cases}$$

Lemma 2.4. *Let $a, b, c, d \in A$ with $p \nmid abcd$. Let $\Phi(a, b)$ and $\Phi(c, d)$ be rank 2 Drinfeld modules over F . Then, the following are equivalent:*

1. *The finite Drinfeld modules over \mathbb{F}_p given by $\phi(\hat{a}, \hat{b})$ and $\phi(\hat{c}, \hat{d})$ are \mathbb{F}_p -isomorphic.*
2. *$\hat{c}\hat{a}^{-1}$ is a perfect $(q-1)^{\text{th}}$ power in \mathbb{F}_p^* , and $(c\hat{a}^{-1})^{(q+1)} \equiv d\hat{b}^{-1} \pmod{p}$*

Proof. This follows directly from [Gek08, §1.4] □

Lemma 2.5. *The number of \mathbb{F}_p -isomorphism classes of rank 2 Drinfeld modules over \mathbb{F}_p containing a representative of the form $\phi(0, \delta)$ for some $\delta \in \mathbb{F}_p$ is $O(q^2)$.*

Proof. The pairs $(0, \delta)$ can be parametrized by \mathbb{F}_p^* , and multiplication by a $(q^2 - 1)^{\text{th}}$ power gives \mathbb{F}_p -isomorphic Drinfeld modules. Therefore our quantity is bounded by

$$\# \left(\mathbb{F}_p^* / (\mathbb{F}_p^*)^{q^2-1} \right) = q^2 - 1.$$

□

2.4. Character sum estimates for Dirichlet characters over A . The first lemma is a straightforward consequence of the Riemann Hypothesis for function fields. We record it, with proof, for the sake of completeness. In particular, we later make use of the explicit dependence of the bound on the degree of the conductor of the character.

Lemma 2.6. *Let $p \in A^{(1)}$ be a prime with $\deg p = x$. Fix natural numbers $z' \leq z \leq x$. Fix a nonprincipal Dirichlet character χ modulo p . Then we have the upper bound*

$$\left| \sum_{\substack{f \in A^{(1)} \\ z' \leq \deg f \leq z}} \chi(f) \right| \leq q^{z/2} 2^x.$$

Proof. We write the L -function $L(s, \chi)$ associated to χ in two different ways and compare coefficients. By definition, for $\text{Re } s > 1$ we have

$$L(s, \chi) = \sum_{f \in A^{(1)}} \chi(f) |f|^{-s}.$$

Under the change of variables $X \leftrightarrow q^{-s}$, and writing

$$c(k) := \sum_{f \in A^{(1)}, \deg f = k} \chi(f),$$

this becomes

$$L(s, \chi) = \sum_{k=1}^x c(k) X^k.$$

Examining the product expansion given in (2.1), we see that $c(k)$ is the k^{th} elementary symmetric polynomial in x letters evaluated at $\{-\alpha_i\}_{i=1}^x$. Ignoring cancellation among summands in this presentation of $c(k)$, we get the upper bound

$$|c(k)| \leq \binom{x}{k} q^{k/2},$$

which immediately yields the bound

$$\left| \sum_{\substack{f \in A^{(1)} \\ z' \leq \deg f \leq z}} \chi(f) \right| \leq q^{z/2} \sum_{k=z'}^z \binom{x}{k}.$$

The lemma follows by completing the sum of binomial coefficients to range from 0 to x . \square

Lemma 2.7. *Let $p \in A^{(1)}$ be a prime. Fix a natural number z . Let $\{a_n\}$ be a sequence of complex numbers supported on $\{n \in A^{(1)} : \deg n \leq z\}$. We have the bound*

$$\sum_{\chi \pmod{p}} \left| \sum_{\substack{n \in A^{(1)} \\ \deg n \leq z}} a_n \chi(n) \right|^2 = \varphi(p) \sum_{\deg f < \deg p} \left| \sum_{\substack{n \in A^{(1)} \\ \deg n \leq z \\ n \equiv f \pmod{p}}} a_n \right|^2,$$

where the sum is taken of all Dirichlet characters mod p .

Proof. Expand the square on the left hand side and use orthogonality of characters. This is essentially the same as [Bai07, Lemma 5]. \square

3. FROM DRINFELD MODULES TO A SUM OF CLASS NUMBERS

Our first task is to remove the dependence on the box size from the calculation; our approach follows [Bai07] and uses character sums to simultaneously treat congruence conditions and isomorphism conditions.

From here on, we fix $a \in A$ and $u \in \mathbb{F}^*$. We assume that $x > 2 \deg a$; the case of equality poses additional complications that would require further study to address. If x is even, then we further assume that $-4u$ is a nonsquare in \mathbb{F}^* . We define I_p to be the number of \mathbb{F}_p isomorphism classes $[\phi]$ of rank 2 Drinfeld modules over \mathbb{F}_p such that:

1. For any representative $\phi(\gamma, \delta)$ of $[\phi]$, $P(\gamma, \delta) = X^2 - aX + up$; and
2. There does not exist a representative of $[\phi]$ of the form $\phi(0, \delta)$.

By Lemma 2.5, we have $H_p - I_p = O(q^2)$.

3.1. Application of character sums estimates. We change the order of summation to obtain

$$\begin{aligned} S(x, \mathcal{A}, \mathcal{B}, a, u) &= \frac{1}{\#\text{Box}(\mathcal{A}, \mathcal{B})} \sum_{p \in \mathcal{P}} \#\{(g, \Delta) \in \text{Box}(\mathcal{A}, \mathcal{B}) : p \nmid \Delta, P_p(X, g, \Delta) = X^2 - aX + up\} \\ &= \frac{1}{\#\text{Box}(\mathcal{A}, \mathcal{B})} \sum_{p \in \mathcal{P}} \#\{(g, \Delta) \in \text{Box}(\mathcal{A}, \mathcal{B}) : p \nmid g\Delta, P_p(X, g, \Delta) = X^2 - aX + up\} + O\left(\frac{q^A}{|p|}\right). \end{aligned}$$

Let $(u_{p,j}, v_{p,j})$ for $j = 1, \dots, I_p$ be pairs of monic elements of A such that

$$\{\phi(\hat{u}_{p,j}, \hat{v}_{p,j})\}_{j=1}^{I_p}$$

forms a system of representatives of \mathbb{F}_p -isomorphism classes of rank 2 Drinfeld modules over \mathbb{F}_p with $P(X, \hat{u}_{p,j}, \hat{v}_{p,j}) = X^2 - aX + up$ and $p \nmid u_{p,j}$. With this notation the expression inside of this last sum becomes

$$(3.1) \quad \sum_{j=1}^{I_{p,a}} \#\{(g, \Delta) \in \text{Box}(\mathcal{A}, \mathcal{B}) : \phi(\hat{g}, \hat{\Delta}) \cong_{\mathbb{F}_p} \phi(\hat{u}_{p,j}, \hat{v}_{p,j})\}$$

By Lemma 2.4, (g, Δ) satisfies the condition in the summand of (3.1) if and only if:

1. $gu_{p,j}^{-1}$ is a perfect $(q-1)^{\text{th}}$ power modulo p , and
2. $(gu_{p,j}^{-1})^{q+1} \equiv \Delta v_{p,j}^{-1} \pmod{p}$.

To detect the first condition, we use the $(q-1)^{\text{th}}$ power residue symbol $(\cdot)_{(q-1)}$. It has properties similar to those of power residue symbols in the classical setting; see [Ros02, Chapter 3] for details. In particular, we have

$$\sum_{k=0}^{q-2} \left(\frac{gu_{p,j}^{-1}}{p} \right)_{(q-1)}^k = \begin{cases} q-1 & \text{if } gu_{p,j}^{-1} \text{ is a perfect } (q-1)^{\text{th}} \text{ power modulo } p, \\ 0 & \text{otherwise.} \end{cases}$$

For the second condition, orthogonality of Dirichlet characters implies that

$$\sum_{\chi \pmod{p}} \chi(g^{q+1} u_{p,j}^{-(q+1)} \Delta^{-1} v_{p,j}) = \begin{cases} \varphi(p) & \text{if } (gu_{p,j}^{-1})^{q+1} \equiv \Delta v_{p,j}^{-1} \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

We now write (3.1) as

$$\frac{1}{(q-1)\varphi(p)} \sum_{j=1}^{I_p} \sum_{(g, \Delta) \in \text{Box}(\mathcal{A}, \mathcal{B})} \left(\sum_{k=0}^{q-2} \left(\frac{gu_{p,j}^{-1}}{p} \right)_{(q-1)}^k \right) \left(\sum_{\chi \pmod{p}} \chi(g^{q+1} u_{p,j}^{-(q+1)} \Delta^{-1} v_{p,j}) \right).$$

For χ a Dirichlet character mod p , and $0 \leq k \leq q-2$, define

$$\begin{aligned} G_1(\chi, k) &:= \sum_{j=1}^{I_p} \left(\frac{u_{p,j}^{-1}}{p} \right)_{(q-1)}^k \chi^{q+1}(u_{p,j}^{-1}) \chi(v_{p,j}), \\ G_2(\chi, k) &:= \sum_{\substack{g \in A^{(1)} \\ \deg g < \mathcal{A}}} \left(\frac{g}{p} \right)_{(q-1)}^k \chi^{q+1}(g), \text{ and} \\ G_3(\chi, k) &:= \sum_{\substack{\Delta \in A^{(1)} \\ \deg \Delta < \mathcal{B}}} \chi(\Delta). \end{aligned}$$

In this notation, (3.1) becomes

$$(3.2) \quad \frac{1}{(q-1)\varphi(p)} \sum_{k=0}^{q-2} \sum_{\chi \pmod{p}} G_1(\chi, k) G_2(\chi, k) G_3(\chi, k).$$

In (3.2), there is exactly one totally trivial term, namely $(\chi, k) = (\chi_0, 0)$. The contribution of this term is

$$\frac{I_p q^{A+B}}{(q-1)\varphi(p)} = \frac{H_p q^{A+B}}{(q-1)|p|} \left(1 + O\left(\frac{1}{|p|}\right) \right) + O\left(\frac{q^{2+A+B}}{(q-1)\varphi(p)}\right).$$

There are two types of semi-trivial terms in (3.2). Suppose first that $\chi \neq \chi_0$ and $(\cdot)_{(q-1)}^k \chi^{q+1} = \chi_0$. This means that $\chi^{q+1} = (\cdot)_{(q-1)}^{-k}$, and there are at most $q+1$ choices of χ satisfying this relation. Altogether, there are at most $O(q^2)$ such terms overall. For each of these terms, we estimate G_1 and G_2 trivially, and bound G_3 using Lemma 2.6. The total contribution of these terms is

$$O\left(\frac{I_p 2^x q^{2+A+(B/2)}}{(q-1)|p|}\right).$$

Now suppose that $\chi = \chi_0$ and $k \neq 0$, which occurs for $O(q)$ terms. Here we estimate G_1 and G_3 trivially, and bound G_2 using Lemma 2.6. The total contribution of these terms is

$$O\left(\frac{I_p 2^x q^{1+(A/2)+B}}{(q-1)|p|}\right).$$

For the remaining terms in (3.2), we apply the Cauchy-Schwarz inequality to obtain

$$\begin{aligned}
 (3.3) \quad & \frac{1}{(q-1)\varphi(p)} \sum_{k=1}^{q-2} \left(\sum_{\substack{\chi \pmod{p}, \chi \neq \chi_0 \\ \chi^{q+1} \neq (\cdot)^{-k}_{(q-1)}}} G_1(\chi, k) G_2(\chi, k) G_3(\chi, k) \right) \ll \\
 & \sum_{k=1}^{q-2} \left(\sum_{\chi \pmod{p}} \left| \sum_{j=1}^{I_p} \left(\frac{u_{p,j}^{-1}}{p} \right)_{(q-1)}^k \chi(u_{p,j}^{-(q+1)} v_{p,j}) \right|^2 \right)^{1/2} \times \\
 & \left(\sum_{\chi \pmod{p}, \chi \neq \chi_0} q \left| \sum_{\substack{g \in A^{(1)} \\ \deg g < \mathcal{A}}} \chi(g) \right|^4 \right)^{1/4} \left(\sum_{\chi \pmod{p}, \chi \neq \chi_0} \left| \sum_{\substack{\Delta \in A^{(1)} \\ \deg \Delta < \mathcal{B}}} \chi(\Delta) \right|^4 \right)^{1/4}
 \end{aligned}$$

The q in the second factor on the right hand side of (3.3) appears since, for fixed χ_1 , there are $O(q)$ choices of χ satisfying $\chi^{q+1} = \chi_1$. The second and third factors on the right hand side of (3.3) are bounded using Lemma 2.6. For the first factor on the right hand side of (3.3), we apply Lemma 2.7, noting that

$$\#\{j : u_{p,j}^{-(q+1)} v_{p,j} \equiv f \pmod{p}\} \leq q$$

for all $f \pmod{p}$, and is nonzero for at most I_p choices of $f \pmod{p}$. Altogether, the contribution from these terms is bounded by

$$O\left(\frac{|p|^{1/2} I_p^{1/2} 4^x q^{(3+\mathcal{A}+\mathcal{B})/2}}{(q-1)|p|}\right).$$

Combining the above estimates, we have

$$S(x, \mathcal{A}, \mathcal{B}, a, u) = \frac{q^{\mathcal{A}+\mathcal{B}}}{\#\text{Box}(\mathcal{A}, \mathcal{B})} \frac{1}{(q-1)q^x} \sum_{p \in \mathcal{P}} H_p + E,$$

where

$$E = O\left(\frac{1}{xq^{\mathcal{B}}} + \frac{1}{q^{2x+1}} \sum_{p \in \mathcal{P}} H_p + \frac{2^x}{q^{x+1}} \left(\frac{q}{q^{\mathcal{A}/2}} + \frac{q^2}{q^{\mathcal{B}/2}}\right) \sum_{p \in \mathcal{P}} H_p + \frac{q^{1/2}}{q^{x/2}} \frac{4^x}{q^{(\mathcal{A}+\mathcal{B})/2}} \sum_{p \in \mathcal{P}} (H_p)^{1/2}\right).$$

From the analytic class formula and a trivial bound on $L(1, \chi)$, we can write

$$H_p \ll x^2 q^{x/2} \text{ and } (H_p)^{1/2} \ll x q^{x/4};$$

this allows us to rewrite E as

$$E = O\left(1 + \frac{q^{x/2}}{(q-1)x} \left(\frac{x^2}{q^{2x+1}} + x^2 2^x \left(\frac{q}{q^{\mathcal{A}/2}} + \frac{q^2}{q^{\mathcal{B}/2}}\right) + \frac{4^x q^{3/2+x/4}}{q^{\mathcal{A}/2+\mathcal{B}/2}}\right)\right)$$

In order for the main term to dominate E as $x \rightarrow \infty$, we require that \mathcal{A} and \mathcal{B} satisfy (1.2).

4. APPLICATION OF THE PRIME NUMBER THEROEM FOR ARITHMETIC PROGRESSIONS

We now focus on the quantity

$$(4.1) \quad \frac{1}{(q-1)q^x} \sum_{p \in \mathcal{P}} H_p,$$

upon observing that

$$\frac{q^{A+B}}{\#\text{Box}(\mathcal{A}, \mathcal{B})} = 1 + \underline{o}(1) \text{ as } q^x \rightarrow \infty.$$

Combining the analogue of Deuring's lemma (Theorem 2.2) with the class number formula (Lemma 2.1), and taking C_∞ as defined in (1.1), we get

$$H_p = (q-1)C_\infty \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up}} \frac{|p|^{1/2}}{|r|} L(1, \chi_R),$$

where $R := R(r, u, a, p) = \frac{a^2 - 4up}{r^2}$. Altogether we rewrite (4.1) as

$$(4.2) \quad \frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up}} \frac{L(1, \chi_R)}{|r|}.$$

We recall an effective version of the prime number theorem for arithmetic progressions. For a proof, see [Ros02, p.40-42], while keeping track of the dependence of the O -constant on m .

Theorem 4.1. *Suppose $m, a \in A$ with $(m, a) = 1$. Then*

$$\#\{p, \deg p = x : p \equiv a \pmod{m}\} = \frac{1}{\varphi(m)} \frac{q^x}{x} + O\left(\frac{(\deg m)^2}{x} q^{x/2}\right).$$

4.1. Sum truncations. We follow the strategy of [DP99], that is, upon expanding the L -value we get a triple sum, truncate in two directions, and control the third direction using Theorem 4.1.

Expressing the L -value as a sum, we rewrite (4.2) as

$$(4.3) \quad \frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up}} \frac{1}{|r|} \sum_{v \in A^{(1)}} \frac{\chi_R(v)}{|v|}.$$

We fix a parameter U , depending on x , to be determined precisely later. We aim to control the contribution of $r \in A^{(1)}$ with $\deg r \geq U$. Changing the order of summation and bounding the L -value trivially, we get that this is

$$\frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r \geq U}} \frac{1}{|r|} \sum_{v \in A^{(1)}} \frac{\chi_R(v)}{|v|} = O\left(\frac{x}{q^{x/2}} \sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{1}{|r|} \#\{p \in \mathcal{P} : r^2 | a^2 - 4up\}\right).$$

Applying Theorem 4.1, we rewrite this as

$$(4.4) \quad O \left(q^{x/2} \sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{1}{|r| \varphi(r^2)} + \sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{(\deg r)^2}{|r|} \right).$$

The second sum in (4.4) is $O(x^3)$. For the first sum in (4.4) we have

$$\sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{1}{|r| \varphi(r^2)} \leq \frac{1}{q^{2U}} \sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{1}{\varphi(r)}.$$

Elementary manipulations give the bound

$$\sum_{\substack{r \in A^{(1)} \\ U \leq \deg r \leq x/2}} \frac{1}{\varphi(r)} \ll x \sum_{\substack{r \in A^{(1)} \text{ sqfree} \\ U \leq \deg r \leq x/2}} \frac{1}{\varphi(r)},$$

as well as

$$\sum_{\substack{r \in A^{(1)} \text{ sqfree} \\ U \leq \deg r \leq x/2}} \frac{1}{\varphi(r)} \ll x.$$

Altogether we have

$$\frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r \geq U}} \frac{1}{|r|} \sum_{v \in A^{(1)}} \frac{\chi_R(v)}{|v|} = O \left(\frac{q^{x/2} x^2}{q^{2U}} + x^3 \right).$$

Therefore, we require that

$$(4.5) \quad U > \varepsilon x \text{ for some } 0 < \varepsilon < 1.$$

We fix a second parameter V , depending on x and to be determined precisely later. Our next task is to control the contribution of $v \in A^{(1)}$ with $\deg v \geq V$. We write this as

$$(4.6) \quad \frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r < U}} \frac{1}{|r|} \sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{\chi_R(v)}{|v|} = O \left(\frac{1}{q^{x/2}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r < U}} \frac{1}{|r|} \sum_{p \in \mathcal{P}} \sum_{y=V}^x \frac{1}{q^y} \sum_{\substack{v \in A^{(1)} \\ \deg v=y}} \chi_R(v) \right).$$

The innermost sum on the right hand side of (4.6) can be bounded as in the proof of Lemma 2.6 by $O \left(q^{y/2} \binom{x-2 \deg r}{y} \right)$. This leaves us with

$$\sum_{y=V}^x \frac{1}{q^y} \sum_{\substack{v \in A^{(1)} \\ \deg v=y}} \chi_R(v) = O \left(\sum_{y=V}^x \frac{1}{q^{y/2}} \binom{x-2 \deg r}{y} \right) = O \left(\frac{2^x}{q^{V/2}} \right).$$

This shows that

$$\sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r < U}} \frac{1}{|r|} \sum_{y=V}^x \frac{1}{q^y} \sum_{\substack{v \in A^{(1)} \\ \deg v = y}} \chi_R(v) = O \left(\frac{2^x}{q^{V/2}} \sum_{\substack{r \in A^{(1)} \\ \deg r < U}} \frac{1}{|r|} \#\{p \in \mathcal{P} : r^2 | a^2 - 4up\} \right).$$

We apply Theorem 4.1 to the inner quantity, and note that

$$\sum_{\substack{r \in A^{(1)} \\ \deg r < U}} \frac{1}{|r| \varphi(r)} = O(1) \text{ and } \sum_{\substack{r \in A^{(1)} \\ \deg r < U}} \frac{(\deg r)^2}{|r|} = O(U^3),$$

and (4.6) becomes

$$\frac{C_\infty}{q^{x/2}} \sum_{p \in \mathcal{P}} \sum_{\substack{r \in A^{(1)} \\ r^2 | a^2 - 4up \\ \deg r < U}} \frac{1}{|r|} \sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{\chi_R(v)}{|v|} = O \left(\frac{2^x}{q^{V/2}} \frac{q^{x/2} + U^3}{x} \right).$$

Therefore, we require that

$$(4.7) \quad V > \left(\frac{\log 4}{\log q} + \varepsilon \right) x \text{ for some } \varepsilon > 0.$$

4.2. Extracting the main term. We are left considering the sum

$$(4.8) \quad \frac{1}{q^{x/2}} \sum_{u \in \mathbb{F}^*} \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U}} \frac{1}{|r|} \sum_{\substack{p \in \mathcal{P} \\ r^2 | a^2 - 4up}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|v|} \chi_R(v).$$

We make some observations leading to conditions in our sum.

- If $r \mid a^2 - 4up$ and $r \mid a$, then $r \mid p$. But $\deg r \leq U$, and U will be chosen strictly less than x , therefore the latter will not happen. This means that we can restrict the sum to a sum over r satisfying

$$(4.9) \quad (r, a) = 1$$

- The value of $\chi_R(v)$ depends R modulo v and not on R itself, and $\gcd(R, v) \neq 1$ implies that $\chi_R(v) = 0$.
- Let σ be a representative for a class in $(A/vA)^*$. Then

$$\frac{a^2 - 4up}{r^2} \equiv \sigma \pmod{v} \iff p \equiv \frac{a^2 - r^2 \sigma}{4u} \pmod{vr^2}.$$

- Observe that $\gcd(\sigma r^2 - a^2, v) = 1$ if and only if $\gcd(\sigma r^2 - a^2, vr^2) = 1$. One direction is obvious. For the other direction, suppose that $\gcd(\sigma r^2 - a^2, v) = 1$ and there exists a prime ℓ such that $\ell \mid vr^2$ and $\ell \mid \sigma r^2 - a^2$. Our hypothesis implies that $\ell \nmid v$, so it is necessary that $\ell \mid r$ and consequentially that $\ell \mid a^2$. This contradicts (4.9).

We introduce the explicit conditions just discussed into (4.8) and partition the inner sum into residue classes to get

We partition into residue classes and explicitly introduce the conditions just discussed to write

$$\frac{1}{q^{x/2}} \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U \\ \gcd(a,r)=1}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|rv|} \sum_{\substack{\sigma(v)^* \\ \gcd(\sigma r^2 - a^2, v)=1}} \chi_\sigma(v) \# \left\{ p, \deg p = x : p \equiv \frac{a^2 - r^2 \sigma}{4u} \pmod{vr^2} \right\},$$

where $*$ indicates that the sum is taken over representatives of $(A/vA)^*$.

We now apply Theorem 4.1. We ensure that $\deg vr^2 < x$ by requiring that

$$(4.10) \quad 2U + V \leq (1 - \varepsilon)x \quad \text{for some } \varepsilon > 0.$$

It follows that

$$\# \left\{ p, \deg p = x : p \equiv \frac{a^2 - r^2 \sigma}{4u} \pmod{vr^2} \right\} = \frac{1}{\varphi(vr^2)} \frac{q^x}{x} + O\left(x^2 q^{x/2}\right).$$

We bound the contribution of the error terms as follows.

$$\begin{aligned} & \frac{1}{q^{x/2}} \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U \\ \gcd(a,r)=1}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|rv|} \sum_{\substack{\sigma(v)^* \\ \gcd(\sigma r^2 - a^2, v)=1}} \chi_\sigma(v) x^2 q^{x/2} \\ &= O \left(x^2 \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U}} \frac{1}{|r|} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|v|} \sum_{\sigma(v)^*} 1 \right) = O(x^4 q^V). \end{aligned}$$

We see that we need

$$(4.11) \quad V \leq x \left(\frac{1}{2} - \varepsilon \right) \quad \text{for some } \varepsilon > 0.$$

We choose U and V as follows. Under the assumption that $q > 16$, we note that

$$\frac{\log 4}{\log q} < \frac{1}{2};$$

provided x is not too small, we can choose

$$U := \left\lfloor \frac{1}{4}x \right\rfloor, V := \left\lceil \left(\frac{1}{4} + \frac{\log 2}{\log q} \right) x \right\rceil$$

and this choice will satisfy (4.5), (4.7), (4.10), and (4.11) as $x \rightarrow \infty$. Our main term, coming from the main term in the prime number theorem, becomes

$$\begin{aligned} & \frac{C_\infty}{q^{x/2}} \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U \\ \gcd(a,r)=1}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|rv|} \sum_{\substack{\sigma(v)^* \\ \gcd(\sigma r^2 - a^2, v)=1}} \chi_\sigma(v) \frac{1}{\varphi(vr^2)} \frac{q^x}{x} \\ (4.12) \quad &= C_\infty \frac{q^{x/2}}{x} \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{1}{|rv| \varphi(vr^2)} \sum_{\substack{\sigma(v)^* \\ \gcd(\sigma r^2 - a^2, v)=1}} \chi_\sigma(v) \end{aligned}$$

5. THE CONSTANT $C(a)$

We introduce the following notation. For $v, r \in A^{(1)}$ with $\gcd(r, a) = 1$, write

$$c(a; v, r) := \sum_{\substack{\sigma(v)^* \\ \gcd(\sigma r^2 - a^2, v) = 1}} \chi_\sigma(v)$$

With this notation, the constant appearing in our the main term of is

$$C_\infty \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{c(a; v, r)}{|rv| \varphi(vr^2)}$$

We first extend this to a sum over all $v, r \in A^{(1)}$ and show that the infinite sum converges, and converges quickly enough so that we can replace the bounded sum in our main term by the infinite sum. Then, we rewrite the infinite sum as a product over primes in A , so that our constant can be more easily compared with those coming from conjectures and other results in the literature.

5.1. Properties of $c(a; v, r)$. Following [DP99], we write explicit expressions for $c(a; v, r)$, giving an upper bound on its absolute value. We first note that $c(a; v, r)$ is multiplicative in v . Indeed, let $\gcd(v_1, v_2) = 1$ and for a fixed $\sigma \pmod{v_1 v_2}$ there are unique $\sigma_1 \pmod{v_1}$ and $\sigma_2 \pmod{v_2}$ such that

$$\sigma = \sigma_1 + k_1 v_1 = \sigma_2 + k_2 v_2 \text{ for some } k_1, k_2 \in A.$$

Moreover,

$$\gcd(\sigma r^2 - a^2, v_1 v_2) = 1 \implies \gcd(\sigma r^2 - a^2, v_1) = 1 \text{ and } \gcd(\sigma r^2 - a^2, v_2) = 1,$$

and for $i = 1, 2$,

$$\gcd(\sigma r^2 - a^2, v_i) = \gcd((\sigma_i + k_i v_i) r^2 - a^2, v_i) = \gcd(\sigma_i r^2 - a^2, v_i).$$

Multiplicativity now follows by splitting the character sum in $c(a; v_1 v_2, r)$.

We now focus on $c(a; \ell^k, r)$ where ℓ is a prime in A . We consider two cases.

If $\gcd(\ell, r) = 1$ then $\sigma \mapsto \sigma r^2$ is a permutation of the set

$$\{\sigma(\ell^k)^* : \gcd(\sigma r^2 - a^2, \ell^k) = 1\}$$

Therefore

$$c(a; \ell^k, r) = \sum_{\substack{\sigma(\ell^k)^* \\ \gcd(\sigma r^2 - a^2, \ell) = 1}} \chi_\sigma(\ell)^k = \sum_{\substack{\hat{\sigma}(\ell^k)^* \\ \gcd(\hat{\sigma} - a^2, \ell) = 1}} \chi_{\hat{\sigma}}(\ell)^k = c(a; \ell^k, 1)$$

But this last quantity is

$$c(a; \ell^k, 1) = |\ell|^{k-1} \left(\left(\sum_{\hat{\sigma}(\ell)^*} \chi_{\hat{\sigma}}(\ell)^k \right) - \chi_{a^2}(\ell)^k \right).$$

If $\ell \nmid a$, this is

$$c(a; \ell^k, 1) = \begin{cases} |\ell|^{k-1}(|\ell| - 2) & \text{if } k \text{ even,} \\ -|\ell|^{k-1} & \text{if } k \text{ odd,} \end{cases}$$

If $\ell \mid a$, this is

$$c(a; \ell^k, 1) = \begin{cases} |\ell|^{k-1}(|\ell| - 1) & \text{if } k \text{ even,} \\ 0 & \text{if } k \text{ odd,} \end{cases}$$

If $\gcd(\ell, r) = \ell$, it follows that $\ell \nmid a$ and the condition $\gcd(\hat{\sigma}r^2 - a^2, \ell) = 1$ is vacuous. Therefore

$$c(a; \ell^k, r) = \sum_{\hat{\sigma}(\ell)^*} \chi_{\hat{\sigma}}(\ell)^k$$

By orthogonality, this is 0 if k is odd and $|\ell|^{k-1}(|\ell| - 1)$ if k is even. The following lemma summarizes this discussion.

Lemma 5.1. *Take the notation above. Then*

$$c(a; \ell^k, r) = \begin{cases} c(a; \ell^k, \ell) & \text{if } \ell \mid r \\ c(a; \ell^k, 1) & \text{if } \ell \nmid r; \end{cases}$$

more precisely,

$$c(a; \ell^k, r) = \begin{cases} |\ell|^{k-1}(|\ell| - 2) & \text{if } k \text{ even, } \ell \nmid a, \ell \nmid r \\ -|\ell|^{k-1} & \text{if } k \text{ odd, } \ell \nmid a, \ell \nmid r \\ |\ell|^{k-1}(|\ell| - 1) & \text{if } k \text{ even, } \ell \mid a, \ell \nmid r \\ 0 & \text{if } k \text{ odd, } \ell \mid a, \ell \nmid r \\ |\ell|^{k-1}(|\ell| - 1) & \text{if } k \text{ even, } \ell \mid r \\ 0 & \text{if } k \text{ odd, } \ell \mid r. \end{cases}$$

Define $\kappa(\cdot)$ as the multiplicative function with values on prime powers given by

$$\kappa(\ell^k) = \begin{cases} 1 & \text{if } k \text{ even,} \\ |\ell| & \text{if } k \text{ odd.} \end{cases}$$

From Lemma 5.1 it is clear that

$$|c(a; \ell^k, r)| \leq \frac{|\ell^k|}{\kappa(\ell^k)}$$

From the multiplicativity of $c(a; v, r)$, we get the following bound.

Corollary 5.2. *Take the notation above. For all $v \in A^{(1)}$,*

$$|c(a; v, r)| \leq \frac{|v|}{\kappa(v)}$$

5.2. Extending the constant to an infinite sum. For fixed r , Corollary 5.2 implies that

$$(5.1) \quad \sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{|c(a; v, r)|}{|v|\varphi(v)} \leq \sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{1}{\kappa(v)\varphi(v)},$$

and we wish to control the growth of this sum as $y \rightarrow \infty$. If $v \in A^{(1)}$ can be written as $v = m^2n$ with $m, n \in A^{(1)}$ and n squarefree, then $\kappa(v)$ is simply $|n|$. With this we rewrite the sum on the right hand side of (5.1) as

$$\sum_{y \geq V} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y/2}} \sum_{\substack{n \in A^{(1)} \text{ sqfree} \\ \deg n = y - 2 \deg m}} \frac{1}{|n|\varphi(m^2n)} = \sum_{y \geq V} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y/2}} \sum_{\substack{n \in A^{(1)} \text{ sqfree} \\ \deg n = y - 2 \deg m}} \frac{1}{|mn|\varphi(mn)},$$

and bound it trivially by

$$\begin{aligned}
O \left(\sum_{y \geq V} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y/2}} \frac{1}{|m|\varphi(m)} \sum_{\substack{n \in A^{(1)} \text{ sqfree} \\ \deg n = y - 2 \deg m}} \frac{1}{|n|\varphi(n)} \right) &= O \left(\sum_{y \geq V} \frac{1}{q^y} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y/2}} \frac{|m|}{\varphi(m)} \sum_{\substack{n \in A^{(1)} \text{ sqfree} \\ \deg n = y - 2 \deg m}} \frac{1}{\varphi(n)} \right) \\
&= O \left(\sum_{y \geq V} \frac{y}{q^y} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y/2}} \frac{|m|}{\varphi(m)} \right)
\end{aligned}$$

We bound φ crudely from below as $\varphi(m) \gg (q-1)^{\deg m}$, using the fact that $q > 2$ since q is an odd prime power. With this bound we get that

$$\frac{|m|}{\varphi(m)} \ll \left(\frac{3}{2}\right)^{\deg m}.$$

Altogether we have

$$\sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{|c(a; v, r)|}{|v|\varphi(v)} = O \left(\sum_{y \geq V} y \frac{\left(\frac{3}{2}\right)^y}{q^{y/2}} \right).$$

Since q is an odd prime power, this sum converges, and we have the bound

$$(5.2) \quad \sum_{\substack{v \in A^{(1)} \\ \deg v \geq V}} \frac{|c(a; v, r)|}{|v|\varphi(v)} = O \left(\frac{1}{\left(\frac{2}{3}q^{1/2}\right)^V} \right)$$

With this, we can bound the sums

$$(5.3) \quad \sum_{\substack{r \in A^{(1)} \\ \gcd(r, a) = 1}} \sum_{\substack{v \in A^{(1)} \\ \deg v > V}} \frac{c(a; v, r)}{|rv|\varphi(vr^2)} \quad \text{and} \quad \sum_{\substack{r \in A^{(1)} \\ \gcd(r, a) = 1 \\ \deg r > U}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{c(a; v, r)}{|rv|\varphi(vr^2)}.$$

For the first sum in (5.3), we use (5.2) as follows:

$$\begin{aligned}
\sum_{\substack{r \in A^{(1)} \\ \gcd(r, a) = 1}} \sum_{\substack{v \in A^{(1)} \\ \deg v > V}} \frac{|c(a; v, r)|}{|rv|\varphi(vr^2)} &\leq \sum_{\substack{r \in A^{(1)} \\ \gcd(r, a) = 1}} \frac{1}{|r|\varphi(r^2)} \sum_{\substack{v \in A^{(1)} \\ \deg v > V}} \frac{|c(a; v, r)|}{|v|\varphi(v)} \\
&\ll \frac{1}{\left(\frac{2}{3}q^{1/2}\right)^V} \sum_{\substack{r \in A^{(1)} \\ \gcd(r, a) = 1}} \frac{1}{|r|\varphi(r^2)}
\end{aligned}$$

The inner sum can be bounded above by

$$\sum_{r \in A^{(1)}} \frac{1}{|r|^2} = O(1).$$

For the second sum in (5.3), we extend the sum over v and note that

$$\sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1 \\ \deg r > U}} \frac{1}{|r|\varphi(r^2)} \sum_{v \in A^{(1)}} \frac{|c(a;v,r)|}{|v|\varphi(v)} \ll \sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1 \\ \deg r > U}} \frac{1}{|r|^2} \ll \frac{1}{q^U}.$$

We record the result of the computations above in the following lemma.

Lemma 5.3. *Take the notation above. Then,*

$$\left| \sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \sum_{v \in A^{(1)}} \frac{c(a;v,r)}{|rv|\varphi(vr^2)} - \sum_{\substack{r \in A^{(1)} \\ \deg r \leq U \\ \gcd(r,a)=1}} \sum_{\substack{v \in A^{(1)} \\ \deg v \leq V}} \frac{c(a;v,r)}{|rv|\varphi(vr^2)} \right| \ll \frac{1}{q^U} + \frac{1}{\left(\frac{2}{3}q^{1/2}\right)^V}$$

In particular, the sums over v and r in (4.12) can be extended to sums over suitable elements of $A^{(1)}$ of all degree, at the cost of an error of

$$O\left(\frac{q^{x/2}}{x} \left(\frac{1}{q^U} + \frac{1}{\left(\frac{2}{3}q^{1/2}\right)^V}\right)\right),$$

and this expression is $\underline{O}\left(\frac{q^{x/2}}{x}\right)$ as $x \rightarrow \infty$.

5.3. Product expansion of the constant. To complete the proof, we rewrite the sum

$$\sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \sum_{v \in A^{(1)}} \frac{c(a;v,r)}{|rv|\varphi(vr^2)},$$

in order to see that it gives rise to $C(a)$ as defined in the statement of Theorem 1.2. The computations needed are elementary and reliant on properties of multiplicative functions. In particular, we follow [DP99, Proof of Lemma 4.1, p. 16-17]

From (1.3) we get

$$\sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \sum_{v \in A^{(1)}} \frac{c(a;v,r)}{|rv|\varphi(vr^2)} = \sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \frac{1}{|r|\varphi(r^2)} \sum_{v \in A^{(1)}} \frac{c(a;v,r)}{|v|\varphi(v)} \frac{\varphi(\gcd(v,r^2))}{|\gcd(v,r^2)|}$$

We expand the inner sum as a product over primes to write

$$\sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \frac{1}{|r|\varphi(r^2)} \prod_{\ell} \left(\sum_{\alpha \geq 0} \frac{c(a;\ell^\alpha, r)}{|\ell^\alpha|\varphi(\ell^\alpha)} \frac{\varphi(\gcd(\ell^\alpha, r^2))}{|\gcd(\ell^\alpha, r^2)|} \right)$$

Whenever $\ell \nmid r$, this last factor vanishes and $c(a;\ell^\alpha, r) = c(a;\ell^\alpha, 1)$, so we extract a product from the sum to get

$$\prod_{\ell} \left(\sum_{\alpha \geq 0} \frac{c(a;\ell^\alpha, 1)}{|\ell^\alpha|\varphi(\ell^\alpha)} \right) \sum_{\substack{r \in A^{(1)} \\ \gcd(r,a)=1}} \frac{1}{|r|\varphi(r^2)} \prod_{\ell|r} \left(\frac{\sum_{\alpha \geq 0} \frac{c(a;\ell^\alpha, r)}{|\ell^\alpha|\varphi(\ell^\alpha)} \frac{\varphi(\gcd(\ell^\alpha, r^2))}{|\gcd(\ell^\alpha, r^2)|}}{\sum_{\alpha \geq 0} \frac{c(a;\ell^\alpha, 1)}{|\ell^\alpha|\varphi(\ell^\alpha)}} \right)$$

The expression inside of this sum is a multiplicative function over r , so we can write the sum as a product over primes $\ell' \nmid a$. Since the product inside of the sum runs over primes dividing r , $r = \ell^\beta$, $\beta \neq 0 \implies \ell' = \ell$. The sum in the denominator gives cancellation in the first product, so we write

$$(5.4) \quad \prod_{\ell|a} \left(\sum_{\alpha \geq 0} \frac{c(a; \ell^\alpha, 1)}{|\ell^\alpha| \varphi(\ell^\alpha)} \right) \prod_{\ell \nmid a} \left(\sum_{\substack{\alpha \geq 0 \\ \beta \geq 0}} \frac{1}{|\ell^\beta| \varphi(\ell^{2\beta})} \frac{c(a; \ell^\alpha, \ell^\beta)}{|\ell^\alpha| \varphi(\ell^\alpha)} \frac{\varphi(\gcd(\ell^\alpha, \ell^{2\beta}))}{|\gcd(\ell^\alpha, \ell^{2\beta})|} \right)$$

This last factor is $1 - \frac{1}{|\ell|}$ if $\alpha\beta \neq 0$ and 1 otherwise. Therefore, the remaining sum becomes

$$\begin{aligned} & \sum_{\substack{\alpha \geq 0 \\ \beta \geq 0}} \frac{1}{|\ell^\beta| \varphi(\ell^{2\beta})} \frac{c(a; \ell^\alpha, \ell^\beta)}{|\ell^\alpha| \varphi(\ell^\alpha)} \frac{\varphi(\gcd(\ell^\alpha, \ell^{2\beta}))}{|\gcd(\ell^\alpha, \ell^{2\beta})|} \\ &= 1 + \sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, 1)}{|\ell^\alpha| \varphi(\ell^\alpha)} + \sum_{\beta \geq 1} \frac{1}{|\ell^\beta| \varphi(\ell^{2\beta})} + \left(1 - \frac{1}{|\ell|}\right) \sum_{\beta \geq 1} \frac{1}{|\ell^\beta| \varphi(\ell^{2\beta})} \sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, \ell)}{|\ell^\alpha| \varphi(\ell^\alpha)} \\ &= 1 + \sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, 1)}{|\ell^\alpha| \varphi(\ell^\alpha)} + \frac{1}{|\ell|^3 - 1} \left(\frac{|\ell|}{|\ell| - 1} + \sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, \ell)}{|\ell^\alpha| \varphi(\ell^\alpha)} \right) \end{aligned}$$

Using Lemma 5.1, we compute the remaining sums:

$$\sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, 1)}{|\ell^\alpha| \varphi(\ell^\alpha)} = \begin{cases} \frac{1}{|\ell|^2 - 1} & \text{if } \ell \mid a \\ \frac{-2}{(|\ell|^2 - 1)(|\ell| - 1)} & \text{if } \ell \nmid a, \end{cases}$$

and

$$\sum_{\alpha \geq 1} \frac{c(a; \ell^\alpha, \ell)}{|\ell^\alpha| \varphi(\ell^\alpha)} = \frac{1}{|\ell|^2 - 1}$$

Returning to 5.4, we now have

$$\prod_{\ell|a} \left(1 + \frac{1}{|\ell|^2 - 1} \right) \prod_{\ell \nmid a} \left(1 - \frac{2}{(|\ell|^2 - 1)(|\ell| - 1)} + \frac{1}{|\ell|^3 - 1} \left(\frac{|\ell|}{|\ell| - 1} + \frac{1}{|\ell|^2 - 1} \right) \right),$$

which simplifies to

$$\prod_{\ell|a} \left(1 - \frac{1}{|\ell|^2} \right)^{-1} \prod_{\ell \nmid a} \left(\frac{|\ell|(|\ell|^2 - |\ell| - 1)}{(|\ell|^2 - 1)(|\ell| - 1)} \right).$$

ACKNOWLEDGEMENTS

The author thanks A. C. Cojocaru for suggesting this problem and for conversations about it, Matei Vlad for helpful suggestions regarding character sum estimates, and an anonymous referee for helpful comments on an earlier version of this paper. This project is part of the author's doctoral thesis at the University of Illinois at Chicago, and was completed while the author was on an Abraham Lincoln Fellowship; the author thanks the Department of Mathematics, Statistics, and Computer Science and the Graduate College at the University of Illinois at Chicago for providing conditions suitable for research.

REFERENCES

- [Art24] E. Artin, *Quadratische krper im gebiete der hheren kongruenzen. i.*, Mathematische Zeitschrift **19** (1924), no. 1, 153–206 (German).
- [Bai07] Stephan Baier, *The Lang-Trotter conjecture on average*, J. Ramanujan Math. Soc. **22** (2007), no. 4, 299–314. MR 2376806 (2008j:11065)
- [BS09] William D. Banks and Igor E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277. MR 2570668 (2011a:11121)
- [CFM05] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty, *The square sieve and the Lang-Trotter conjecture*, Canad. J. Math. **57** (2005), no. 6, 1155–1177. MR 2178556 (2006e:11074)
- [Cha08] Mei-Chu Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. **145** (2008), no. 3, 409–442. MR 2462111 (2009i:11099)
- [Dav96] Chantal David, *Average distribution of supersingular Drinfel’d modules*, J. Number Theory **56** (1996), no. 2, 366–380. MR 1373559 (96j:11080)
- [DL63] H. Davenport and D. J. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) **12** (1963), 129–136. MR 0167482 (29 #4755)
- [DP99] Chantal David and Francesco Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices (1999), no. 4, 165–183. MR 1677267 (2000g:11045)
- [Dri74] V. G. Drinfel’d, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656. MR 0384707 (52 #5580)
- [Dri77] ———, *Elliptic modules. II*, Mat. Sb. (N.S.) **102(144)** (1977), no. 2, 182–194, 325. MR 0439758 (55 #12644)
- [FM96] Etienne Fouvry and M. Ram Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), no. 1, 81–104. MR 1382477 (97a:11084)
- [Gek91] Ernst-Ulrich Gekeler, *On finite Drinfel’d modules*, J. Algebra **141** (1991), no. 1, 187–203. MR 1118323 (92e:11064)
- [Gek08] ———, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721. MR 2366959 (2008m:11114)
- [LT76] Serge Lang and Hale Trotter, *Frobenius distributions in GL_2 -extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976, Distribution of Frobenius automorphisms in GL_2 -extensions of the rational numbers. MR 0568299 (58 #27900)
- [MMS88] M. Ram Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281. MR 935007 (89d:11036)
- [Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657 (2003d:11171)
- [Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559 (83k:12011)
- [Yu95] Jiu-Kang Yu, *A class number relation over function fields*, J. Number Theory **54** (1995), no. 2, 318–340. MR 1354056 (96i:11128)

DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S MORGAN ST, 322 SEO, CHICAGO, 60607, IL, USA.

E-mail address: abel65535@gmail.com